IN THE CLAIMS:

Please cancel Claims 22 to 29, and amend Claims 1 to 5, 8 and 10 to 12 as shown below. The claims, as pending in the subject application, now read as follows:

---

1. (Currently amended) A method for the secure printing of print data from a client application residing on a data network to an interface device which has a printer, said interface device residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said method comprising the steps of:

generating print data in said client application;

determining whether [[a]] secure communication paths exist ~~path exists~~ between said client application and said cable head end, and between said cable head end and said interface device;

C1

transmitting, in response to a determination that said secure communication paths exist ~~path exists~~, said print data from said client application to said interface device; and

sending said print data from said interface device to said printer for printing.

2. (Currently amended) A method according to Claim 1, wherein the step for determining whether said secure communication paths exist ~~path exists~~ between said client application and said interface device includes the use of a secure protocol between said client application and said cable head end, and between said cable head end and said interface device.

3. (Currently amended) A method according to Claim 2, wherein the step for determining whether said secure communication paths exist ~~path exists~~ between said client application and said interface device further includes a confirmation through said secure protocol, that said cable head end is a secure location, and a confirmation, through said secure protocol, that said interface device is a secure location.

4. (Currently amended) A method according to Claim 1, wherein the step for transmitting, in response to a determination that said secure communication paths exist ~~path exists~~, said print data from said client application to said interface device includes sending said print data from said client application to said cable head end in a device-independent format, transforming said print data from said device-independent format to a rasterized format which corresponds to said printer, and then sending said print data in said rasterized format from said cable head end to said interface device for printing on said printer.

C1

5. (Currently amended) A method according to Claim 1, wherein the step for transmitting, in response to a determination that said secure communication paths exist ~~path exists~~, said print data from said client application to said interface device includes encrypting said print data, sending said encrypted print data from said client application to said cable head end, sending said encrypted print data from said cable head end to said interface device, decrypting said print data, and sending the decrypted print data to said printer for printing.

6. (Previously presented) A method according to Claim 3, wherein said confirmation that said interface device is a secure location is sent from said interface device to said cable head end.

7. (Original) A method according to Claim 3, wherein said confirmation that said cable head end is a secure location is sent from said cable head end to said client application.

8. (Currently amended) A method according to Claim 1, wherein the step for transmitting, in response to a determination that said secure communication paths exist ~~path exists~~, said print data from said client application to said interface device includes transforming, by said client application, said print data from said device-independent format to a rasterized format which corresponds to said printer, sending said print data in said rasterized format from said client application to said cable head end, and then sending said print data in said rasterized format from said cable head end to said interface device for printing on said printer.

9. (Original) A method according to Claim 2, wherein said secure protocol is a secure sockets layer protocol.

10. (Currently amended) A method according to Claim 2, wherein the step for determining whether said secure communication paths exist ~~path exists~~ between said client application and said interface device includes the transmission of at least one

certificate from said interface device to said cable head end and the transmission of at least one certificate from said cable head end to said client application.

Not amended 11. (Currently amended) A method for the secure printing of print data from a client application residing on a data network to an interface device which has a printer, said interface device residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said method comprising the steps of;

C1

generating print data in said client application;

determining that a secure communication path exists between said client application and said cable head end upon receipt through a secure protocol of a confirmation from said cable head end that said cable head end is a secure location;

sending, in response to a determination that said secure communication path exists, said print data from said client application to said cable head end in a device-independent format;

transforming in said cable head end, said print data from said device-independent format to a rasterized format which corresponds to said printer;

determining that a secure communication path exists between said cable head <ins>end</ins> and said interface device upon receipt, through a secure protocol, of a confirmation from said interface device that said interface device is a secure location; and

sending, in response to a determination that said secure communication path exists, said print data in said rasterized format from said cable head end to said interface device for printing on said printer.

12. (Currently amended) A method for the secure printing of print data from a client application residing on a data network to an interface device which has a printer, said interface device residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said method comprising the steps of:

generating print data in said client application;

transforming, in said client application, said print data from <u>a</u> [[said]] device-independent format to a rasterized format which corresponds to said printer;

C1 encrypting, in said client application, said print data in said rasterized format;

sending said encrypted print data in said rasterized format from said client application to said cable head end;

sending said encrypted print data in said rasterized format from said cable head end to said interface device; and

decrypting, in said interface device, said print data in said rasterized format for printing on said printer.

13. (Previously presented) An apparatus for the secure printing of print data from a client application residing on a data network to an interface device which has a printer, said interface device residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, comprising:

a program memory for storing process steps executable to perform a method according to any of Claims 1 to 12; and

a processor for executing the process steps stored in said program memory.

14. (Previously presented) Computer-executable process steps stored on a computer readable medium, said computer-executable process steps for the secure printing of print data from a client application residing on a data network to an interface device which has a printer, said interface device residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 12.

15. (Previously presented) A computer-readable medium which stores computer-executable process steps, the computer-executable process steps to achieve the secure printing of print data from a client application residing on a data network to an interface device which has a printer, said interface device residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 12.

16. (Previously presented) A method according to Claim 1, wherein said interface device is a set top box.

17. (Previously presented) A method according to Claim 11, wherein said interface device is a set top box.

18. (Previously presented) A method according to Claim 12, wherein said interface device is a set top box.

19. (Previously presented) An apparatus according to Claim 13, wherein said interface device is a set top box.

20. (Previously presented) Computer-executable process steps according to Claim 14, wherein said interface device is a set top box.

21. (Previously presented) A computer-readable medium according to Claim 15, wherein said interface device is a set top box.

22. to 29. Canceled.